PATENT ABSTRACTS OF JAPAN

JP

(11)Publication number : 2001-014239

(43)Date of publication of application : 19.01.2001

(51)Int.Cl.. G06F 13/00
G06F 12/14
G06F 15/00

(21)Application number : 11-182908

(22)Date of filing : 29.06.1999

(71)Applicant : HITACHI LTD

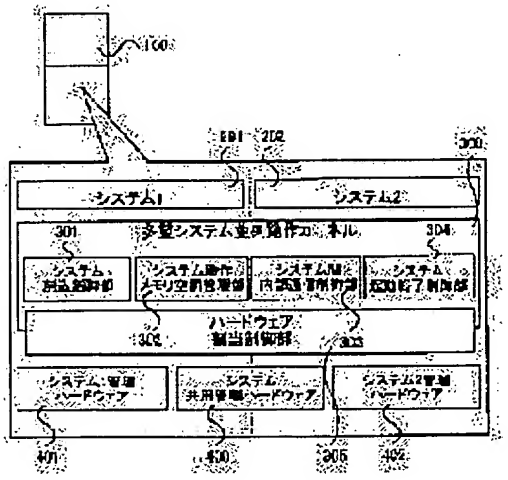
(72)Inventor : FURUKAWA HIROSHI
SHINOHARA DAISUKE
OSHIMA SATOSHI
UCHIYAMA YASUFUMI

(54) SECURITY SYSTEM BY MULTIPLEX SYSTEM PARALLEL OPERATED COMPUTERS

(57)Abstract:

PROBLEM TO BE SOLVED: To secure the security of systems to be simultaneously and parallel operated without altering the systems by making a monitoring system monitor the contents of inter-system communications with the other system and an illegal inter-system communication control from the other system and preventing the influence of an illegal intrusion and control when an illegality is detected except for the monitoring system.

SOLUTION: A multiplex system parallel operation kernel 300 simultaneously and parallel operates plural systems on one computer. A system interruption control part 301 controls the interruption between respective systems and performs assigning or scheduling of processors. Besides, a system operation memory space managing part 302 manages the memories of respective systems and assigns memories for each of respective systems. When an illegal access is performed from one system to the multiplex system parallel operation kernels 300, the multiplex system parallel operation kernel 300 enables a general system itself to stop while using a system start/end control part 304.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]In environment where information is delivered by other systems and intersystem communications by a supervising system which is at least one system taking the lead by a computer which carries out simultaneous parallel operation of two or more systems on one computer, The contents of intersystem communication with a system of at least others [supervising system / said], Certification information and unjust intersystem communication control from other systems are supervised, A security system by a multiplex system parallel operation computer when [said] supervising system detection is carried out [performed / except said supervising system / an unjust invasion or unjust control], wherein influence of an unjust invasion and control does not attain to said supervising system at least.
[Claim 2]A security system by a multiplex system parallel operation computer, wherein two or more system action environment where it operates on one computer operates in claim 1 in an environment which completely became independent.
[Claim 3]A security system by a multiplex system parallel operation computer being able to assign two or more systems which operate on one computer in claim 1 as hardware to which each manages hardware which exists on one computer at the time of computer starting.
[Claim 4]A security system by a multiplex system parallel operation computer, wherein communication between two or more systems which operate on one computer is possible and access restriction can set it to intersystem communication inside said apparatus by intersystem communication inside apparatus in claim 1.
[Claim 5]When an unjust invasion and unjust control are performed to one system in claim 1, A security system by a multiplex system parallel operation computer which ends and resets without reset of an apparatus power supply only a system by which said unauthorized entry and control were performed, and is characterized by influence not attaining to other systems.
[Claim 6]Via a public circuit at least to one computer for relay of a system which performs communications control. Use a computer in which two or more systems of claim 1 carry out simultaneous parallel operation, and the inner 1 ** of two or more of said systems becomes a supervising system, and supervises other systems, Provide environment which connected a supervising system to an internal circuit and other systems connected to an external public circuit, respectively, and said provided environment, To a system connected to a public circuit at least by using the feature of claims 1, 2, 3, 4, and 5, an unjust invasion from

the outside, A security system by a multiplex system parallel operation computer being able to provide environment of safety where influence of said unjust invasion, control, and an attack does not reach in an internal circuit even when control and an attack are delivered.

[Claim 7]A security system by a multiplex system parallel operation computer, wherein a public circuit of claim 6 includes the Internet, intranet, and extranet at least.

[Claim 8]A security system by a multiplex system parallel operation computer by which a firewall and a packet converter being included at least in a computer for relay of claim 6.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the security system provided by the computer which can carry out simultaneous parallel operation of two or more systems on a single computer.
[0002]The communications control security at the time of accessing a public circuit including especially the Internet, intranet, and extranet into a specific site from the client on said public circuit in the network used as a backbone circuit is included at least.
[0003]
[Description of the Prior Art]a former and single computer top -- if -- in order to carry out unitary control of the hardware, it was common that one system operated. Even when comparing and working two or more systems, it was made to operate as a virtual computer like JP,7-129419,A, and, as for hardware control/resource control, the base system of the virtual machine was performing all. Therefore, a possibility that security will be easily broken by unjust invasion/operation to a base system was high.
[0004]A public circuit including especially the Internet, intranet, and extranet in the network used as a backbone circuit. It was common to have used the computer machines which combined a single system or single system apparatus in the communications control at the time of accessing into a specific site from the client on said public circuit as a security translator for communications controls. That is, security reservation of said computer for translators was an important technical problem in the same system.
[0005]
[Problem(s) to be Solved by the Invention]In this invention, the environment where simultaneous parallel operation of two or more systems is carried out on a single computer is used, and the security of the systems which are carrying out simultaneous parallel operation is secured, without converting the system itself. According to this invention, the security of mutual systems, Even when the supervising system which controls the original multiplex system parallel operation kernel which moves by a base, and said multiplex system parallel operation kernel takes charge and unjust invasion is carried out to one system, the security which does not have influence in other systems is provided. Even when it invades into the system of one metaphor from the outside and unlawful access is able to be tried via said kernel, ending the system itself accessed when the supervising system checked the operation etc. offers the purpose environment where the secondary influence of the system on others is prevented.

[0006]In the network which uses the public circuit which includes the Internet, intranet, and extranet which are increasing by leaps and bounds now by using the aforementioned security especially as a backbone circuit, It is also at least one purpose to provide the communications control security function at the time of accessing into a specific site from the client of said public circuit point. It realizes, when said two or more systems use the computer in which simultaneous parallel operation is possible for the computer for translators generally used by said communications control now and specifically carry out security reservation to it.

[0007]

[Means for Solving the Problem]A means for realizing an aforementioned problem is explained using drawing 1.

[0008]In the first place, this invention has a means to carry out simultaneous parallel operation of two or more systems on one computer. A 300 multiplex-system parallel operation kernel of drawing 1 provides said means. A 301 system interruption control section controls interruption between each system, and, specifically, performs assignment and scheduling of a processor. The 302 system-action memory space Management Department manages a memory of each system, and performs memory assignment for every system. That is, a multiplex system parallel operation kernel (300) is completely [each system] controllable, and when unlawful access is performed from one system to a multiplex system parallel operation kernel (300), a stop of the general-purpose system itself of it is also attained using a 304 system-startup end controlling part.

[0009]It exists on one computer the second, and has a means to conceal hardware which is carrying out original management for every system from other systems. A 305 hardware quota system part of drawing 1 provides said means. A hardware quota system part (305) manages hardware (401 and 402) which each system manages uniquely, and hardware (400) which a system has by common use, It becomes possible to dissociate from other systems and to conceal hardware which has a function which assigns each hardware to each system at the time of starting, and one system has with said function.

[0010]It has a means to control communication between two or more systems which carry out simultaneous parallel operation on one computer to the third. An interior communication control section between 303 systems in a 300 multiplex-system parallel operation kernel of drawing 1 provides said means. Uniquely, the interior communication control section between 303 systems can provide a function between mutual systems which communicates, and can also provide a function to provide access restriction in communication between systems as occasion demands without communication to the computer exterior, such as a network.

[0011]One system which operates on one computer can be realized without reconstruction of security which does not have on other systems of the system itself using the above means, It is available as a system of a translator which provides an advanced communications control security function at the time of accessing into a specific site from a client of the public circuit point.

[0012]

[Embodiment of the Invention]One example of this invention is described using a drawing.

[0013]Drawing 1 is a figure explaining the system configuration of this invention. 100 is one computer. 201 and 202 are systems which operate on a computer (100), and are an operating system (OS) which exists

in a world at least, and the software for computing control containing middle software. 300 is a multiplex system parallel operation kernel which operates on a computer (100), and is a system for operating two or more said systems (201, 202) on one computer. In a multiplex system parallel operation kernel (300), a 301 system interruption control section, the 302 system-action memory space Management Department, the interior communication control section between 303 systems, and a 304 system-startup end controlling part exist. In a multiplex system parallel operation kernel (300), one function of the 305 hardware quota system part which manages the hardware which exists in a computer and enables hardware assignment for every system exists. 401 is the hardware in the computer (100) managed by the system 1 (201), and 402 is the hardware in the computer (100) managed by the general-purpose system 2 (202). On the other hand, 400 is hardware which all the systems which exist in a computer (100) use by common use. In this example, in order to explain simply, the system which operates within one computer (100) was set to two, but these can be existed by more than one.

[0014]A multiplex system parallel operation kernel (300) rises at the time of computer (100) starting, and fixes the environment for operating two or more systems (201, 202). The 302 system-action memory space Management Department assigns required memory space for every system, and loading of each system of it is attained on the assigned memory space. A 301 system interruption control section assigns the processor which each system uses at the time of starting. Of course, this assignment is a case where two or more processors exist in a computer (100), and when there is only one processor, a system interruption control section (301) manages the interruption scheduling of an after-starting processor, and it controls to pass processing to each system if needed.

[0015]Operation becomes possible, without simultaneous-standing in a row as mentioned above, and moreover two or more systems in an one computer top adding change and reconstruction independently to the system itself.

[0016]A hardware quota system part (305) also functions as a part of multiplex system parallel operation kernel (300) at the time of computer (100) starting, and the hardware (401, 402) which each system manages uniquely, and the hardware (400) used by common use are assigned. When hardware carries out information acquisition from a system (201, 202) accessible in an after-starting user, System 1 management hardware (401) and system common management hardware (400) can acquire the system 2 management hardware (402) from the system 2 (202), and system common management hardware (400) from the system 1 (201). That is, in the system 2 (202), in the hardware information and the system 1 (201) which the self-system has not managed, the information on system 1 management hardware (401) cannot detect system 2 management hardware (402), and even the existence can detect it no longer.

[0017]By using the function explained above, two or more computer environment which completely became independent is realizable on one computer.

[0018]A multiplex system parallel operation kernel (300) carries out agency control of the interior communication between two or more systems which operate on it. This is realized by the interior communication control section between 303 systems. In order that said interior communication may not disseminate information to the exterior at all, compared with actually communicating among two or more computers, that the communication content is intercepted has high safety few. Since it is only that a communications interface appears from a system, unless the structure of a multiplex system parallel

operation kernel (300) is known, there are also few possibilities that the communication content will be decoded. It is also possible to set up access restriction by communication between systems if needed. For example, when communicating by the system 1 (201) and the system 2 (202), communication of only the demand from the system 2 (202) and its response is permitted, and the needed information from the system 1 (201) can also perform setting out which is disregarded. The case where there is injustice of access restriction from the system 1 (201) when the above-mentioned access restriction is set up, When it is detected by the system 2 (202) side that unjust operation/control are performed by the inaccurate invader on the system 1 (201), where a computer (100) is started, it also becomes possible through a 304 general-purpose system startup end controlling part to perform an end and reboot of the system 1 (201).

[0019]Also when an inaccurate invader performs unjust operation/control by taking composition like drawing 1 to the system which operates on a computer as I understand by the above explanation, high correspondence of safety is always attained.

[0020]Next, drawing 4 explains the example of 1 use of this invention from drawing 2. However, this is an example of 1 use to the last, and here where various security effects are induced by taking the same composition is possible for it.

[0021]Drawing 2 is a figure showing the composition of the communications control at the time of accessing a public circuit including the Internet, intranet, and extranet which are generally used now into a specific site from the client on said public circuit in the network used as a backbone circuit.

[0022]The composition contents of drawing 2 are explained. 1000 is an external client computer. Interface hardware for 1001 to communicate an external client computer (1000). A LAN board/card, a modem, etc. are mentioned as a general example. The system by which 1002 works on an external client computer (1000). 1003 is client software which operates on said system (1002). The public line whose 2000 is a channel of a demand/reply packet of said client software (1003). The specific site in which said client software (1003) is the destination about a demand/reply packet 3000. The network site closed as an example in the internal network of the company is mentioned, and said site holds both access points of the internal network in a public line (2000) and a company. 3100 is a public line (2000) in a specific site (3000), and a network for security located in the middle of the internal network in a specific site (3000), and is generally called a boundary network. 3110 is between a public line (2000) and a boundary network (3100), is information machines and equipment which filter the communication packet which goes a mutual network back and forth, and is generally called an external router. The external<-> boundary communication control part which 3111 is an external router (3110) and actually provides the filtering function of a packet. The boundary server computer which 3120 has on a boundary network (3100) and performs a justification check and attestation of the communication from client software (1003). Interface hardware for 3121 to communicate a boundary server computer (3120). The system by which 3122 works on a boundary server computer (3120). 3123 is server software which operates on said system (3122), and is called a boundary server. The client specification processing corresponding point which 3124 performs a justification check and attestation of the communication from client software (1003) on said boundary server (3123), and transmits a processing packet to the internal network of a specific site (3000) as occasion demands. 3200 is an internal network in a specific site (3000). 3210 is between a boundary network (3100) and an internal network (3200), is information machines and equipment which filter the

communication packet which goes a mutual network back and forth, and is generally called an internal router. The internal<-> boundary communication control part which 3211 is an external router (3210) and actually provides the filtering function of a packet. The internal server computer which 3220 has in an internal network and performs internal processing etc. in response to processing of the client in an internal network (3200), etc., and the processing from the client specification processing corresponding point (3124) on a boundary server computer (3120). 3230 is an internal client computer in an internal network (3200). In this invention, in order to explain simply, the computer was written with very little composition, but many apparatus which plays the same role as the case of being actual exists.

[0023]Next, a communications processing flow in case an external client computer (1000) accesses to the internal network (3200) in a specific site (3000) is explained using drawing 3. Processing is started by 4000. By 4001, the client software (1003) on an external client computer (1000) publishes the processing request packet to a specific site (3000). Although the final address of said processing request packet is the internal server computer (3220) and internal client computer (3230) on an internal network (3200), the packet request destination actually published is a boundary server computer (3120) on a boundary network (3100). By 4002, the processing request packet which the external client computer (1000) published is sent to an external router (3110) via a public circuit (2000). The processing request packet by which packet filtering of the external<-> boundary communication control part (3111) in an external router (3110) was performed, the address and the packet kind were judged, and justification was checked by 4003 is sent to a boundary server computer (3120). Here, processing is ended when the justification of a packet is inaccurate (4010).

[0024]The processing request packet which reached the boundary server computer (3120) in 4004, It is sent to the boundary server (3123) in a boundary server computer (3120), and by a client specification processing corresponding point (3124). If check of the contents of a packet and attestation of delivery origin are performed and justification is checked, in order to newly send to an internal network (3200) from a client specification processing corresponding point (3124), packet conversion and required authenticating processing are performed and a packet sends to an internal router (3210). Here, processing is ended when attestation of case [where the justification of the contents of a packet is inaccurate], and delivery origin goes wrong (4010). The packet by which packet filtering of the internal<-> boundary communication control part (3211) in an internal router (3210) was performed, the packet kind after conversion was judged, or the check of the address was performed, and justification was checked by 4005 is sent in an internal network.

[0025]On the other hand, processing will be ended, if a packet kind is inaccurate or an address check goes wrong (4010). By 4006, the packet which arrived at the internal network (3200) is sent to the internal server computer (3220) and internal client computer (3230) which perform processing eventually, and a processing demand is performed. The above is a series of communications processing flows in case an external client computer (1000) accesses to the internal network (3200) in a specific site (3000).

[0026]Here, the problem of the security in the composition of drawing 2 is described.

[0027]Generally, encryption of the contents, etc. are given, and the packet which flows through the inside of a public circuit (2000) and the network of a specific site (3100, 3200) is safely designed, even when tapping etc. are encountered comparatively. However, the system (3122) which operates as a base of the boundary server (3123) which exists on a boundary network (3100) generally comprises a circulation OS

and middle software, and the internal structure is easy to be analyzed. As a role of a boundary server (3123), The information from outside is processed and also the security level of the external router (3110) is inevitably set up low in the meaning with the duty which disseminates information outside of filtering of a packet compared with the internal router (3210) in many cases. Therefore, it is easy for an external inaccurate invader to try the unjust invasion to the boundary server computer (3120) on a boundary network (3100), or to send in an inaccurate analysis program.

[0028]When it is accessed illegally or an unjust program is sent in, the analysis and an alteration of the contents of a processing request packet sent, and also the analysis and the alteration of a packet which are sent to an internal network are performed. And the internal networks in a company etc. are eventually allowed invasion, sending of disclosure, a virus, etc. of extra sensitive information etc. is performed, and it suffers serious damage in many cases. Of course, as the measure, it is also possible to work considering the system (3122) on the boundary server computer (3120) of a boundary network (3100) as an original system. However, applications including the server which operates on a system in that case also need to prepare a completely original thing, and flexibility falls remarkably.

[0029]In order to solve the problem on said security, the lineblock diagram at the time of being adapted for the boundary server computer (3120) on a boundary network (3100) in the system configuration of this invention explained by drawing 1 is shown in drawing 4.

[0030]The composition contents of drawing 4 are explained. 1000, 1001, 1002, 1003, 2000, 3000, 3100, 3110, 3111, 3120, 3121, 3122, 3122, 3123, 3124, 3200, 3210, 3211, 3220, and 3230 are together with the composition explained by drawing 2. 300 is the multiplex system parallel operation kernel explained by drawing 1. The client specification processing demand preserving part which is a storing region for 3125 to save temporarily the processing request packet from an external client (1000). Interface hardware for 3126 to perform communication with an internal server computer (3220) on a boundary server computer (3120). The supervising system with which 3127 performs contents supervision of a client specification processing demand preserving part, and the unfair operation/invasion monitoring of a system (3122). Interface hardware for 3321 to communicate an internal server computer (3220). The system by which 3222 works on an internal server computer (3220). 3223 is server software which operates on said system (3222), and is called an internal server. The client specification processing demand acquisition part from which 3224 acquires the processing request packet from [from a client specification processing demand preserving part (3125)] an external client (1000) with directions of a supervising system (3127). The client specification processing internal network corresponding point for 3225 receiving a processing request packet from a client specification processing demand acquisition part, and sending a processing request packet to the specification computer in an internal network. Interface hardware for 3226 to perform communication with a boundary server computer (3120) on an internal server computer (3220). Exclusive gateway LAN which is a network with which 3300 connects the communication-interface hardware (3326) of an internal server computer (3220), and the communication-interface hardware (3126) of a boundary server computer (3120).

[0031]The feature of this composition just adopted as the boundary server computer (3120) the multiplex system operation kernel (300) explained by drawing 1. Said multiplex system operation kernel (300) loads a supervising system (3127) besides the same system (3122) as usual at the time of boundary server

computer (3120) starting. These are realized in the system interruption control section (301) and system memory space management department (302) which were explained by drawing 1. moreover -- although said each system is operating on one computer -- a system (3122) -- a boundary network (3100) -- a supervising system (3127) -- exclusive gateway LAN (3300) -- it is completely connected with the separate network, respectively. The communication-interface hardware (3121, 3126) which each system manages also in hardware is constituted so that hardware information by the side of other systems cannot be detected. This is realized in the hardware quota system part (305) explained by drawing 1. That is, the computer which completely has a separate security level constitutes the environment intermingled independently from on one computer.

[0032]A supervising system (3127) is a multiplex system parallel kernel (300) course, and supervises the system (3122) side periodically. For this reason, as for the needed information from a reverse system (3122), the multiplex system parallel kernel (300) has performed setting out which is not received, although the needed information and the answer from a supervising system (3127) permit access. This is realized by the interior communication control section between systems explained by drawing 1. If it seems that the system (3122) side has received, the processing request packet from an external client (1000), A supervising system (3127) sends directions to an internal server computer (3220) via exclusive gateway LAN (3300), an internal server computer (3220) acquires a processing request packet, and a processing request packet is eventually sent to the specification computer in an internal network.

[0033]When an inaccurate person invades into the system (3122) on a boundary server computer (3120) or an unjust program etc. are sent in, Also when a supervising system (3127) detects and also unlawful access is tried by the multiplex system parallel kernel (300), A multiplex system parallel operation kernel (300) detects, and it is notified to a supervising system (3127), and the end/reboot by the side of a system (3122) are performed by directions of a supervising system (3127), and an administrator is notified of the notice. This is realized by the system startup end controlling part (304) explained by drawing 1.

[0034]A communications processing flow in case the external client computer (1000) using the composition of drawing 4 accesses drawing 5 to the internal network (3200) in a specific site (3000) is explained. Since processing until a processing request packet is sent to a boundary server computer (3120) is the same as that of drawing 3, explanation after it is given here. Processing is started by 5000. The processing request packet which reached the boundary server computer (3120) in 5001, It is sent to the boundary server (3123) in a boundary server computer (3120), and by a client specification processing corresponding point (3124). When check of the contents of a packet and attestation of delivery origin are performed and justification is checked, it is stored in a client specification processing demand preserving part (3125) from a client specification processing corresponding point (3124). Here, processing is ended when attestation of case [where the justification of the contents of a packet is inaccurate], and delivery origin goes wrong (5010). A supervising system (3127) by 5002 via a multiplex system parallel operation kernel (300), When a client specification processing demand preserving part (3125) is checked and a processing request packet exists, if it is a just packet, by checking the contents of a packet via exclusive gateway LAN (3300), Directions of packet acquiring are taken out to the client specification processing demand acquisition part on an internal server (3223). Here, processing is ended when the justification of the contents is inaccurate (5010). By 5003, from a client specification processing demand preserving part (3125), a client

specification processing demand acquisition part acquires a processing packet, and sends the packet to a client specification processing internal network corresponding point (3225). By 5004, a client specification processing internal network corresponding point (3225) sends to the internal server computer (3220) and internal client computer (3230) which perform processing eventually, and a processing demand is performed. External client computers (1000) when the above uses the system configuration of this patent are a series of communications processing flows when accessing to the internal network (3200) in a specific site (3000).

[0035]Explanation of one example of this invention is finished above.

[0036]

[Effect of the Invention]This invention uses the environment where simultaneous parallel operation of two or more systems is carried out on a single computer, and secures without reconstruction of the system itself the security of the systems which are carrying out simultaneous parallel operation. Even when unjust invasion is carried out to the system of one metaphor, reservation of the security which performs a system's own end/reboot into which it was invaded, prevents the secondary influence of the system on others, and does not have on other systems is possible.

[0037]A public circuit including especially the Internet, intranet, and extranet in the network used as a backbone circuit. In the communications control at the time of accessing into a specific site, security reservation of said ******** for communications controls is attained from the client on said public circuit.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Field of the Invention]This invention relates to the security system provided by the computer which can carry out simultaneous parallel operation of two or more systems on a single computer.
[0002]The communications control security at the time of accessing a public circuit including especially the Internet, intranet, and extranet into a specific site from the client on said public circuit in the network used as a backbone circuit is included at least.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention]This invention uses the environment where simultaneous parallel operation of two or more systems is carried out on a single computer, and secures without reconstruction of the system itself the security of the systems which are carrying out simultaneous parallel operation. Even when unjust invasion is carried out to the system of one metaphor, reservation of the security which performs a system's own end/reboot into which it was invaded, prevents the secondary influence of the system on others, and does not have on other systems is possible.
[0037]A public circuit including especially the Internet, intranet, and extranet in the network used as a backbone circuit. In the communications control at the time of accessing into a specific site, security reservation of said ******** for communications controls is attained from the client on said public circuit.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention]In this invention, the environment where simultaneous parallel operation of two or more systems is carried out on a single computer is used, and the security of the systems which are carrying out simultaneous parallel operation is secured, without converting the system itself. According to this invention, the security of mutual systems, Even when the supervising system which controls the original multiplex system parallel operation kernel which moves by a base, and said multiplex system parallel operation kernel takes charge and unjust invasion is carried out to one system, the security which does not have influence in other systems is provided. Even when it invades into the system of one metaphor from the outside and unlawful access is able to be tried via said kernel, ending the system itself accessed when the supervising system checked the operation etc. offers the purpose environment where the secondary influence of the system on others is prevented.
[0006]In the network which uses the public circuit which includes the Internet, intranet, and extranet which are increasing by leaps and bounds now by using the aforementioned security especially as a backbone circuit, It is also at least one purpose to provide the communications control security function at the time of accessing into a specific site from the client of said public circuit point. It realizes, when said two or more systems use the computer in which simultaneous parallel operation is possible for the computer for translators generally used by said communications control now and specifically carry out security reservation to it.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem]A means for realizing an aforementioned problem is explained using drawing 1.

[0008]In the first place, this invention has a means to carry out simultaneous parallel operation of two or more systems on one computer. A 300 multiplex-system parallel operation kernel of drawing 1 provides said means. A 301 system interruption control section controls interruption between each system, and, specifically, performs assignment and scheduling of a processor. The 302 system-action memory space Management Department manages a memory of each system, and performs memory assignment for every system. That is, a multiplex system parallel operation kernel (300) is completely [each system] controllable, and when unlawful access is performed from one system to a multiplex system parallel operation kernel (300), a stop of the general-purpose system itself of it is also attained using a 304 system-startup end controlling part.

[0009]It exists on one computer the second, and has a means to conceal hardware which is carrying out original management for every system from other systems. A 305 hardware quota system part of drawing 1 provides said means. A hardware quota system part (305) manages hardware (401 and 402) which each system manages uniquely, and hardware (400) which a system has by common use, It becomes possible to dissociate from other systems and to conceal hardware which has a function which assigns each hardware to each system at the time of starting, and one system has with said function.

[0010]It has a means to control communication between two or more systems which carry out simultaneous parallel operation on one computer to the third. An interior communication control section between 303 systems in a 300 multiplex-system parallel operation kernel of drawing 1 provides said means. Uniquely, the interior communication control section between 303 systems can provide a function between mutual systems which communicates, and can also provide a function to provide access restriction in communication between systems as occasion demands without communication to the computer exterior, such as a network.

[0011]One system which operates on one computer can be realized without reconstruction of security which does not have on other systems of the system itself using the above means, It is available as a system of a translator which provides an advanced communications control security function at the time of accessing into a specific site from a client of the public circuit point.

[0012]

[Embodiment of the Invention]One example of this invention is described using a drawing.

[0013]Drawing 1 is a figure explaining the system configuration of this invention. 100 is one computer. 201 and 202 are systems which operate on a computer (100), and are an operating system (OS) which exists in a world at least, and the software for computing control containing middle software. 300 is a multiplex system parallel operation kernel which operates on a computer (100), and is a system for operating two or more said systems (201, 202) on one computer. In a multiplex system parallel operation kernel (300), a 301 system interruption control section, the 302 system-action memory space Management Department, the interior communication control section between 303 systems, and a 304 system-startup end controlling part exist. In a multiplex system parallel operation kernel (300), one function of the 305 hardware quota system part which manages the hardware which exists in a computer and enables hardware assignment for every system exists. 401 is the hardware in the computer (100) managed by the system 1 (201), and 402 is the hardware in the computer (100) managed by the general-purpose system 2 (202). On the other hand, 400 is hardware which all the systems which exist in a computer (100) use by common use. In this example, in order to explain simply, the system which operates within one computer (100) was set to two, but these can be existed by more than one.

[0014]A multiplex system parallel operation kernel (300) rises at the time of computer (100) starting, and fixes the environment for operating two or more systems (201, 202). The 302 system-action memory space Management Department assigns required memory space for every system, and loading of each system of it is attained on the assigned memory space. A 301 system interruption control section assigns the processor which each system uses at the time of starting. Of course, this assignment is a case where two or more processors exist in a computer (100), and when there is only one processor, a system interruption control section (301) manages the interruption scheduling of an after-starting processor, and it controls to pass processing to each system if needed.

[0015]Operation becomes possible, without simultaneous-standing in a row as mentioned above, and moreover two or more systems in an one computer top adding change and reconstruction independently to the system itself.

[0016]A hardware quota system part (305) also functions as a part of multiplex system parallel operation kernel (300) at the time of computer (100) starting, and the hardware (401, 402) which each system manages uniquely, and the hardware (400) used by common use are assigned. When hardware carries out information acquisition from a system (201, 202) accessible in an after-starting user, System 1 management hardware (401) and system common management hardware (400) can acquire the system 2 management hardware (402) from the system 2 (202), and system common management hardware (400) from the system 1 (201). That is, in the system 2 (202), in the hardware information and the system 1 (201) which the self-system has not managed, the information on system 1 management hardware (401) cannot detect system 2 management hardware (402), and even the existence can detect it no longer.

[0017]By using the function explained above, two or more computer environment which completely became independent is realizable on one computer.

[0018]A multiplex system parallel operation kernel (300) carries out agency control of the interior communication between two or more systems which operate on it. This is realized by the interior communication control section between 303 systems. In order that said interior communication may not

disseminate information to the exterior at all, compared with actually communicating among two or more computers, that the communication content is intercepted has high safety few. Since it is only that a communications interface appears from a system, unless the structure of a multiplex system parallel operation kernel (300) is known, there are also few possibilities that the communication content will be decoded. It is also possible to set up access restriction by communication between systems if needed. For example, when communicating by the system 1 (201) and the system 2 (202), communication of only the demand from the system 2 (202) and its response is permitted, and the needed information from the system 1 (201) can also perform setting out which is disregarded. The case where there is injustice of access restriction from the system 1 (201) when the above-mentioned access restriction is set up, When it is detected by the system 2 (202) side that unjust operation/control are performed by the inaccurate invader on the system 1 (201), where a computer (100) is started, it also becomes possible through a 304 general-purpose system startup end controlling part to perform an end and reboot of the system 1 (201).

[0019]Also when an inaccurate invader performs unjust operation/control by taking composition like drawing 1 to the system which operates on a computer as I understand by the above explanation, high correspondence of safety is always attained.

[0020]Next, drawing 4 explains the example of 1 use of this invention from drawing 2. However, this is an example of 1 use to the last, and here where various security effects are induced by taking the same composition is possible for it.

[0021]Drawing 2 is a figure showing the composition of the communications control at the time of accessing a public circuit including the Internet, intranet, and extranet which are generally used now into a specific site from the client on said public circuit in the network used as a backbone circuit.

[0022]The composition contents of drawing 2 are explained. 1000 is an external client computer. Interface hardware for 1001 to communicate an external client computer (1000). A LAN board/card, a modem, etc. are mentioned as a general example. The system by which 1002 works on an external client computer (1000). 1003 is client software which operates on said system (1002). The public line whose 2000 is a channel of a demand/reply packet of said client software (1003). The specific site in which said client software (1003) is the destination about a demand/reply packet 3000. The network site closed as an example in the internal network of the company is mentioned, and said site holds both access points of the internal network in a public line (2000) and a company. 3100 is a public line (2000) in a specific site (3000), and a network for security located in the middle of the internal network in a specific site (3000), and is generally called a boundary network. 3110 is between a public line (2000) and a boundary network (3100), is information machines and equipment which filter the communication packet which goes a mutual network back and forth, and is generally called an external router. The external<-> boundary communication control part which 3111 is an external router (3110) and actually provides the filtering function of a packet. The boundary server computer which 3120 has on a boundary network (3100) and performs a justification check and attestation of the communication from client software (1003). Interface hardware for 3121 to communicate a boundary server computer (3120). The system by which 3122 works on a boundary server computer (3120). 3123 is server software which operates on said system (3122), and is called a boundary server. The client specification processing corresponding point which 3124 performs a justification check and attestation of the communication from client software (1003) on said boundary

server (3123), and transmits a processing packet to the internal network of a specific site (3000) as occasion demands. 3200 is an internal network in a specific site (3000). 3210 is between a boundary network (3100) and an internal network (3200), is information machines and equipment which filter the communication packet which goes a mutual network back and forth, and is generally called an internal router. The internal<-> boundary communication control part which 3211 is an external router (3210) and actually provides the filtering function of a packet. The internal server computer which 3220 has in an internal network and performs internal processing etc. in response to processing of the client in an internal network (3200), etc., and the processing from the client specification processing corresponding point (3124) on a boundary server computer (3120). 3230 is an internal client computer in an internal network (3200). In this invention, in order to explain simply, the computer was written with very little composition, but many apparatus which plays the same role as the case of being actual exists.

[0023]Next, a communications processing flow in case an external client computer (1000) accesses to the internal network (3200) in a specific site (3000) is explained using drawing 3. Processing is started by 4000. By 4001, the client software (1003) on an external client computer (1000) publishes the processing request packet to a specific site (3000). Although the final address of said processing request packet is the internal server computer (3220) and internal client computer (3230) on an internal network (3200), the packet request destination actually published is a boundary server computer (3120) on a boundary network (3100). By 4002, the processing request packet which the external client computer (1000) published is sent to an external router (3110) via a public circuit (2000). The processing request packet by which packet filtering of the external<-> boundary communication control part (3111) in an external router (3110) was performed, the address and the packet kind were judged, and justification was checked by 4003 is sent to a boundary server computer (3120). Here, processing is ended when the justification of a packet is inaccurate (4010).

[0024]The processing request packet which reached the boundary server computer (3120) in 4004, It is sent to the boundary server (3123) in a boundary server computer (3120), and by a client specification processing corresponding point (3124). If check of the contents of a packet and attestation of delivery origin are performed and justification is checked, in order to newly send to an internal network (3200) from a client specification processing corresponding point (3124), packet conversion and required authenticating processing are performed and a packet sends to an internal router (3210). Here, processing is ended when attestation of case [where the justification of the contents of a packet is inaccurate], and delivery origin goes wrong (4010). The packet by which packet filtering of the internal<-> boundary communication control part (3211) in an internal router (3210) was performed, the packet kind after conversion was judged, or the check of the address was performed, and justification was checked by 4005 is sent in an internal network.

[0025]On the other hand, processing will be ended, if a packet kind is inaccurate or an address check goes wrong (4010). By 4006, the packet which arrived at the internal network (3200) is sent to the internal server computer (3220) and internal client computer (3230) which perform processing eventually, and a processing demand is performed. The above is a series of communications processing flows in case an external client computer (1000) accesses to the internal network (3200) in a specific site (3000).

[0026]Here, the problem of the security in the composition of drawing 2 is described.

[0027]Generally, encryption of the contents, etc. are given, and the packet which flows through the inside

of a public circuit (2000) and the network of a specific site (3100, 3200) is safely designed, even when tapping etc. are encountered comparatively. However, the system (3122) which operates as a base of the boundary server (3123) which exists on a boundary network (3100) generally comprises a circulation OS and middle software, and the internal structure is easy to be analyzed. As a role of a boundary server (3123), The information from outside is processed and also the security level of the external router (3110) is inevitably set up low in the meaning with the duty which disseminates information outside of filtering of a packet compared with the internal router (3210) in many cases. Therefore, it is easy for an external inaccurate invader to try the unjust invasion to the boundary server computer (3120) on a boundary network (3100), or to send in an inaccurate analysis program.

[0028]When it is accessed illegally or an unjust program is sent in, the analysis and an alteration of the contents of a processing request packet sent, and also the analysis and the alteration of a packet which are sent to an internal network are performed. And the internal networks in a company etc. are eventually allowed invasion, sending of disclosure, a virus, etc. of extra sensitive information etc. is performed, and it suffers serious damage in many cases. Of course, as the measure, it is also possible to work considering the system (3122) on the boundary server computer (3120) of a boundary network (3100) as an original system. However, applications including the server which operates on a system in that case also need to prepare a completely original thing, and flexibility falls remarkably.

[0029]In order to solve the problem on said security, the lineblock diagram at the time of being adapted for the boundary server computer (3120) on a boundary network (3100) in the system configuration of this invention explained by drawing 1 is shown in drawing 4.

[0030]The composition contents of drawing 4 are explained. 1000, 1001, 1002, 1003, 2000, 3000, 3100, 3110, 3111, 3120, 3121, 3122, 3122, 3123, 3124, 3200, 3210, 3211, 3220, and 3230 are together with the composition explained by drawing 2. 300 is the multiplex system parallel operation kernel explained by drawing 1. The client specification processing demand preserving part which is a storing region for 3125 to save temporarily the processing request packet from an external client (1000). Interface hardware for 3126 to perform communication with an internal server computer (3220) on a boundary server computer (3120). The supervising system with which 3127 performs contents supervision of a client specification processing demand preserving part, and the unfair operation/invasion monitoring of a system (3122). Interface hardware for 3321 to communicate an internal server computer (3220). The system by which 3222 works on an internal server computer (3220). 3223 is server software which operates on said system (3222), and is called an internal server. The client specification processing demand acquisition part from which 3224 acquires the processing request packet from [from a client specification processing demand preserving part (3125)] an external client (1000) with directions of a supervising system (3127). The client specification processing internal network corresponding point for 3225 receiving a processing request packet from a client specification processing demand acquisition part, and sending a processing request packet to the specification computer in an internal network. Interface hardware for 3226 to perform communication with a boundary server computer (3120) on an internal server computer (3220). Exclusive gateway LAN which is a network with which 3300 connects the communication-interface hardware (3326) of an internal server computer (3220), and the communication-interface hardware (3126) of a boundary server computer (3120).

[0031]The feature of this composition just adopted as the boundary server computer (3120) the multiplex system operation kernel (300) explained by drawing 1. Said multiplex system operation kernel (300) loads a supervising system (3127) besides the same system (3122) as usual at the time of boundary server computer (3120) starting. These are realized in the system interruption control section (301) and system memory space management department (302) which were explained by drawing 1. moreover -- although said each system is operating on one computer -- a system (3122) -- a boundary network (3100) -- a supervising system (3127) -- exclusive gateway LAN (3300) -- it is completely connected with the separate network, respectively. The communication-interface hardware (3121, 3126) which each system manages also in hardware is constituted so that hardware information by the side of other systems cannot be detected. This is realized in the hardware quota system part (305) explained by drawing 1. That is, the computer which completely has a separate security level constitutes the environment intermingled independently from on one computer.

[0032]A supervising system (3127) is a multiplex system parallel kernel (300) course, and supervises the system (3122) side periodically. For this reason, as for the needed information from a reverse system (3122), the multiplex system parallel kernel (300) has performed setting out which is not received, although the needed information and the answer from a supervising system (3127) permit access. This is realized by the interior communication control section between systems explained by drawing 1. If it seems that the system (3122) side has received, the processing request packet from an external client (1000), A supervising system (3127) sends directions to an internal server computer (3220) via exclusive gateway LAN (3300), an internal server computer (3220) acquires a processing request packet, and a processing request packet is eventually sent to the specification computer in an internal network.

[0033]When an inaccurate person invades into the system (3122) on a boundary server computer (3120) or an unjust program etc. are sent in, Also when a supervising system (3127) detects and also unlawful access is tried by the multiplex system parallel kernel (300), A multiplex system parallel operation kernel (300) detects, and it is notified to a supervising system (3127), and the end/reboot by the side of a system (3122) are performed by directions of a supervising system (3127), and an administrator is notified of the notice. This is realized by the system startup end controlling part (304) explained by drawing 1.

[0034]A communications processing flow in case the external client computer (1000) using the composition of drawing 4 accesses drawing 5 to the internal network (3200) in a specific site (3000) is explained. Since processing until a processing request packet is sent to a boundary server computer (3120) is the same as that of drawing 3, explanation after it is given here. Processing is started by 5000. The processing request packet which reached the boundary server computer (3120) in 5001, It is sent to the boundary server (3123) in a boundary server computer (3120), and by a client specification processing corresponding point (3124). When check of the contents of a packet and attestation of delivery origin are performed and justification is checked, it is stored in a client specification processing demand preserving part (3125) from a client specification processing corresponding point (3124). Here, processing is ended when attestation of case [where the justification of the contents of a packet is inaccurate], and delivery origin goes wrong (5010). A supervising system (3127) by 5002 via a multiplex system parallel operation kernel (300), When a client specification processing demand preserving part (3125) is checked and a processing request packet exists, if it is a just packet, by checking the contents of a packet via exclusive gateway LAN (3300),

Directions of packet acquiring are taken out to the client specification processing demand acquisition part on an internal server (3223). Here, processing is ended when the justification of the contents is inaccurate (5010). By 5003, from a client specification processing demand preserving part (3125), a client specification processing demand acquisition part acquires a processing packet, and sends the packet to a client specification processing internal network corresponding point (3225). By 5004, a client specification processing internal network corresponding point (3225) sends to the internal server computer (3220) and internal client computer (3230) which perform processing eventually, and a processing demand is performed. External client computers (1000) when the above uses the system configuration of this patent are a series of communications processing flows when accessing to the internal network (3200) in a specific site (3000).

[0035]Explanation of one example of this invention is finished above.

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The system configuration figure of this invention.
[Drawing 2]The lineblock diagram of the present public circuit **********.
[Drawing 3]The flow chart of the present public circuit ******** control management.
[Drawing 4]The lineblock diagram at the time of using this invention for public circuit **********.
[Drawing 5]The flow chart of the public circuit ******** control management by this invention.
[Description of Notations]
100 [-- Multiplex system parallel operation kernel,] -- A computer, 201 -- Systems 1 and 202 -- Systems 2 and 300 301 -- A system interruption control section, 302 -- System action memory space Management Department, 303 [-- System common management hardware, 401 / -- System 1 management hardware, 402 / -- System 2 management hardware.] -- The interior communication control section between systems, 304 -- A system startup end controlling part, 305 -- A hardware quota system part, 400

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－14239
（P2001－14239A）
(43)公開日　平成13年１月19日(2001.1.19)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ 13/00	３５１	Ｇ０６Ｆ 13/00	３５１Ｚ　５Ｂ０１７
12/14	３１０	12/14	３１０Ａ　５Ｂ０８５
			３１０Ｋ　５Ｂ０８９
15/00	３２０	15/00	３２０Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全９頁）

(21)出願番号　特願平11－182908

(22)出願日　平成11年６月29日(1999.6.29)

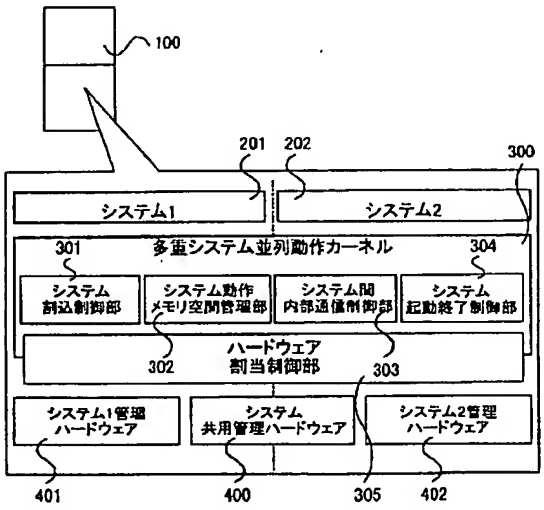
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　古川　博
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　篠原　大輔
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　多重システム並列稼働計算機によるセキュリティシステム

(57)【要約】
【課題】主たる課題は、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造をすることなく確保する。
【解決手段】一台の計算機上で動作する１つのシステムが他のシステムに影響を及ぼさないセキュリティがシステム自体を改造無しで実現可能とし、公共回線先のクライアントから特定サイト内へアクセスをする際の高度な通信制御セキュリティ機能を提供する中継器のシステムとして利用可能である。

図1



【特許請求の範囲】
【請求項１】一台の計算機上で複数のシステムを同時並列稼働する計算機で、少なくとも一つのシステムである監視システムが中心になり、他のシステムとシステム間通信により情報を受け渡しする環境において、前記監視システムが、少なくとも他のシステムとのシステム間通信の内容、認証情報、および他のシステムからの不正なシステム間通信制御の監視を行い、前記監視システム以外で不正な侵入や不正な制御が行われたことを前記監視システム検知した場合には、少なくとも前記監視システムには不正の侵入、制御の影響が及ばないことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項２】請求項１において、一台の計算機上で動作する複数のシステム動作環境は、全く独立した環境で動作することを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項３】請求項１において、一台の計算機上で動作する複数のシステムは、計算機起動時に一台の計算機上に存在するハードウェアを、各々が管理するハードウェアとして割当が可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項４】請求項１において、一台の計算機上で動作する複数のシステム間の通信は、機器内部のシステム間通信により可能であり、前記機器内部のシステム間通信にはアクセス制限が設定可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項５】請求項１において、一つのシステムに不正な侵入や不正な制御が行われた場合、機器電源のリセット無しに、前記不正侵入、制御が行われたシステムのみ終了、リセットし、他のシステムには影響が及ばないことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項６】少なくとも公共回線経由で、通信制御を行うシステムの一台の中継用計算機に、請求項１の複数のシステムが同時並列稼働する計算機を使用し、前記複数のシステムの内１つが監視システムとなり他のシステムを監視し、監視システムは内部の回線に、他のシステムは外部の公共回線に、それぞれ接続した環境を提供し、前記提供された環境は、請求項１、２、３、４，５の特長を利用することにより、少なくとも公共回線に接続するシステムに外部からの不正な侵入、制御、攻撃が行われた場合にでも、内部の回線内には前記不正な侵入、制御、攻撃の影響が及ばない、安全の環境が提供可能であることを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項７】請求項６の公共回線は、少なくともインタネット、イントラネット、エクストラネットを含むことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【請求項８】請求項６の中継用計算機には、少なくともファイアウォール、パケット変換器を含むことを特徴とする、多重システム並列稼働計算機によるセキュリティシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、単一計算機上で複数のシステムを同時並列稼働することが可能な計算機により提供されるセキュリティシステムに関する。
【０００２】特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御セキュリティを少なくとも含む。
【０００３】
【従来の技術】従来、単一計算機上ではハードウェアを一元制御するため、１つのシステムが動作するのが一般的であった。また例え、複数のシステムを稼働する場合でも、特開平７－１２９４１９号の様に仮想的計算機として動作させ、ハードウェア制御/資源管理は仮想計算機のベースシステムが全てを実行していた。そのため、ベースシステムへの不正な侵入/操作などにより容易にセキュリティが破られる可能性が高かった。
【０００４】特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークで、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御においては、単一のシステム、もしくは単一システム機器同士を組み合わせるなどした計算機器類を、通信制御用のセキュリティ中継器として使用することが一般的であった。つまり前記中継器用計算機のセキュリティ確保が同システムでの重要な課題であった。
【０００５】
【発明が解決しようとする課題】本発明では、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造をすることなく確保する。本発明によれば、互いのシステム同士のセキュリティは、ベースで動く独自な多重システム並列稼働カーネルと前記多重システム並列稼働カーネルを制御する監視システムが受け持ち、１つのシステムに不正な侵入がされた場合でも、他のシステムに影響がないセキュリティを提供する。また、例え１つのシステムに外部から侵入し、前記カーネル経由で不正アクセスを試みられた場合でも、その操作を監視システムが確認した時点でアクセスを行ったシステム自身を終了するなど、他のシステムへの二次的な影響を防止する環境の提供も目的とする。
【０００６】特に前記のセキュリティを利用することで、現在飛躍的に増大しているインターネット、イント

ラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線先のクライアントから特定サイト内へアクセスをする際の通信制御セキュリティ機能を提供することも、少なくとも一つの目的である。具体的には、前記通信制御で現在一般的に利用されている中継器用計算機に、前記複数のシステムが同時並列動作可能な計算機を利用し、セキュリティ確保をすることにより実現する。

【０００７】

【課題を解決するための手段】上記課題を実現するための手段を、図１を用い説明する。

【０００８】本発明は第一に、一台の計算機上で複数のシステムを同時並列稼働させる手段を有する。図１の３００多重システム並列稼働カーネルが前記手段を提供する。具体的には、３０１システム割込制御部が、各システム間での割込を制御し、プロセッサーの割当てやスケジューリングを行う。また、３０２システム動作メモリ空間管理部が各システムのメモリを管理し、各システム毎のメモリ割当を行う。つまり多重システム並列稼働カーネル(３００)は各システムの完全に制御可能であり、１つのシステムから多重システム並列稼働カーネル(３００)へ不正アクセスが行われる場合には、３０４システム起動終了制御部を使って、汎用システム自体の停止も可能となる。

【０００９】第二に、一台の計算機上に存在し、システム毎に独自管理しているハードウェアを他のシステムから隠蔽する手段を有する。図１の３０５ハードウェア割当制御部が前記手段を提供する。ハードウェア割当制御部(３０５)は、各システムが独自に管理するハードウェア(４０１および４０２)やシステムが共用で持つハードウェア(４００)を管理し、起動時に各ハードウェアを各システムに割当てる機能を有し、前記機能により一方のシステムが有するハードウェアを他のシステムから分離し、隠蔽する事が可能となる。

【００１０】第三に、一台の計算機上で同時並列稼働する複数のシステム間での通信を制御する手段を有する。図１の３００多重システム並列稼働カーネル内の３０３システム間内部通信制御部が前記手段を提供する。３０３システム間内部通信制御部は、ネットワークなど計算機外部への通信無しで、独自にお互いのシステム間の通信する機能を提供し、必要によりシステム間の通信にアクセス制限を設ける機能も提供可能である。

【００１１】以上の手段を用い、一台の計算機上で動作する１つのシステムが他のシステムに影響を及ぼさないセキュリティがシステム自体の改造無しで実現可能であり、公共回線先のクライアントから特定サイト内へアクセスをする際の高度な通信制御セキュリティ機能を提供する中継器のシステムとして利用可能である。

【００１２】

【発明の実施の形態】本発明の一実施例を、図面を用いて説明する。

【００１３】図１は、本発明のシステム構成を説明した図である。１００は一台の計算機である。２０１、２０２は計算機(１００)上で動作するシステムであり、少なくとも世の中に存在するオペレーティングシステム(ＯＳ)、ミドルソフトを含む計算機制御用ソフトウェアである。３００は計算機(１００)上で動作する多重システム並列動作カーネルであり、前記システム(２０１、２０２)を一台の計算機上で複数動作させるためのシステムである。多重システム並列動作カーネル(３００)内には、３０１システム割込制御部、３０２システム動作メモリ空間管理部、３０３システム間内部通信制御部、３０４システム起動終了制御部が存在する。また、多重システム並列動作カーネル(３００)内には、計算機内に存在するハードウェアを管理し、各システム毎のハードウェア割当を可能にする、３０５ハードウェア割当制御部の一機能が存在する。４０１はシステム１(２０１)によって管理されている計算機(１００)内のハードウェアであり、４０２は汎用システム２(２０２)によって管理されている計算機(１００)内のハードウェアである。一方、４００は計算機(１００)内に存在する全てのシステムが共用で使用するハードウェアである。なお、本実施例では説明を簡単にするため、一台の計算機(１００)内で動作するシステムは２つとしたが、これらは複数存在することが可能である。

【００１４】多重システム並列動作カーネル(３００)は、計算機(１００)起動時に立ち上がり、複数のシステム(２０１、２０２)を動作させるための環境を整備する。３０２システム動作メモリ空間管理部が、各システム毎に必要なメモリ空間の割当を行い、割当てられたメモリ空間上でそれぞれのシステムがロード可能になる。また、３０１システム割込制御部は、各システムが使用するプロセッサーの割当てを起動時に行う。無論この割当は複数のプロセッサーが計算機(１００)内に存在する場合であり、１つのプロセッサーしかない場合は、システム割込制御部(３０１)が起動後プロセッサーの割込スケジューリングを管理し、必要に応じ各システムに処理を渡すように制御を行う。

【００１５】以上の様にして、一台の計算機上で複数のシステムが同時並列かつ独立して、しかもシステム自体に変更や改造を加えることなく動作可能になる。

【００１６】またハードウェア割当制御部(３０５)も、多重システム並列動作カーネル(３００)の一部として計算機(１００)起動時に機能し、各システムが独自に管理するハードウェア(４０１、４０２)、共用で使用するハードウェア(４００)の割当を行う。起動後ユーザがアクセス可能なシステム(２０１、２０２)から、ハードウェアの情報取得した場合、システム１(２０１)からはシステム１管理ハードウェア(４０１)とシステム共用管理ハードウェア(４００)が、システム２(２０２)からはシス

テム２管理ハードウェア（４０２）とシステム共用管理ハードウェア（４００）が取得可能である。つまり自システムが管理していないハードウェア情報、システム１（２０１）ではシステム２管理ハードウェア（４０２）、システム２（２０２）ではシステム１管理ハードウェア（４０１）の情報は、その存在すら検知できないようになる。

【００１７】以上説明してきた機能を利用することで、まったく独立した複数の計算機環境を一台の計算機上に実現可能である。

【００１８】多重システム並列動作カーネル（３００）は、その上で動作する複数のシステム間の内部通信を仲介制御する。これは３０３システム間内部通信制御部で実現する。前記内部通信は全く外部に対して情報を発信しないため、実際に複数の計算機間で通信をすることに比べ、その通信内容が盗聴されたりすることは少なく安全性が高い。また通信用インタフェースがシステムから見えるのみなので、多重システム並列動作カーネル（３００）の構造が分からない限り、その通信内容を解読される可能性も少ない。更に必要に応じて、システム間の通信でアクセス制限を設定する事も可能である。例えば、システム１（２０１）とシステム２（２０２）で通信を行う場合、システム２（２０２）からの要求とその応答のみの通信を許可し、システム１（２０１）からの通信要求は無視するような設定を施すことも可能である。もし上記アクセス制限を設定した場合、システム１（２０１）からアクセス制限の不正があった場合や、不正な侵入者によりシステム１（２０１）上で不正な操作/制御などが行われることをシステム２（２０２）側で検知した場合、３０４汎用システム起動終了制御部を通じ、計算機（１００）を起動した状態で、システム１（２０１）の終了や再起動を行うことも可能となる。

【００１９】以上の説明で分かる通り、図１の様な構成を取ることで、計算機上で動作するシステムに対し不正な侵入者が不正な操作/制御を行った場合にも、常に安全性の高い対応が可能になる。

【００２０】次に本発明の一使用例を図２から図４で説明する。ただし、これはあくまでも一使用例であり、同様な構成を取ることで様々のセキュリティ効果を生むことは可能である。

【００２１】図２は、現在一般的に使用されているインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークにおいて、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御の構成を示した図である。

【００２２】図２の構成内容について説明を行う。１０００は外部クライアント計算機。１００１は外部クライアント計算機（１０００）の通信を行うためのインタフェースハードウェア。一般的な例として、ＬＡＮボード/カード、モデム等が挙げられる。１００２は外部クライアント計算機（１０００）上で稼働するシステム。１００３は前記システム（１００２）上で動作するクライアントソフトウェアである。２０００は前記クライアントソフトウェア（１００３）の要求/返答パケットの通信路である、公衆回線。３０００は前記クライアントソフトウェア（１００３）が要求/返答パケットを送り先である特定サイト。例として企業の内部ネットワークで閉じられたネットワークサイトが挙げられ、前記サイトは公衆回線（２０００）と企業内の内部ネットワークのアクセスポイントの両方を保持する。３１００は特定サイト（３０００）内にある公衆回線（２０００）と特定サイト（３０００）内の内部ネットワークの中間に位置するセキュリティ用ネットワークで、一般的には境界ネットワークと呼ばれる。３１１０は、公衆回線（２０００）と境界ネットワーク（３１００）の間にあり、互いのネットワークを行き来する通信パケットのフィルタリングを行う情報機器で、一般的には外部ルータと呼ばれる。３１１１は外部ルータ（３１１０）で、実際にパケットのフィルタリング機能を提供する外部<;->;境界通信制御部。３１２０は境界ネットワーク（３１００）上に有り、クライアントソフトウェア（１００３）からの通信の正当性確認や認証を行う境界サーバ計算機。３１２１は境界サーバ計算機（３１２０）の通信を行うためのインタフェースハードウェア。３１２２は境界サーバ計算機（３１２０）上で稼働するシステム。３１２３は前記システム（３１２２）上で動作するサーバソフトウェアであり、境界サーバと呼ばれる。３１２４は前記境界サーバ（３１２３）上で、クライアントソフトウェア（１００３）からの通信の正当性確認や認証を行い、必要により特定サイト（３０００）の内部ネットワークに処理パケットを送信するクライアント指定処理対応部。３２００は特定サイト（３０００）内の内部ネットワーク。３２１０は境界ネットワーク（３１００）と内部ネットワーク（３２００）の間にあり、互いのネットワークを行き来する通信パケットのフィルタリングを行う情報機器で、一般的には内部ルータと呼ばれる。３２１１は外部ルータ（３２１０）で、実際にパケットのフィルタリング機能を提供する内部<;->;境界通信制御部。３２２０は内部ネットワーク内にあり、内部ネットワーク（３２００）内のクライアントなどの処理や、境界サーバ計算機（３１２０）上のクライアント指定処理対応部（３１２４）からの処理を受けて内部処理などを実行する内部サーバ計算機。３２３０は内部ネットワーク（３２００）内の内部クライアント計算機。なお本発明では説明を簡単にするため、計算機を極めて少ない構成で書いたが、実際の場合同じ様な役割を果たす多くの機器が存在する。

【００２３】次に図３を使って、外部クライアント計算機（１０００）が、特定サイト（３０００）内の内部ネットワーク（３２００）へアクセスする場合の通信処理流れを説明する。４０００で処理が開始される。４００１で、

外部クライアント計算機（１０００）上のクライアントソフトウェア（１００３）が、特定サイト（３０００）への処理要求パケットを発行する。前記処理要求パケットの最終的な宛先は、内部ネットワーク（３２００）上の内部サーバ計算機（３２２０）や内部クライアント計算機（３２３０）なのだが、実際に発行されるパケット要求先は境界ネットワーク（３１００）上の境界サーバ計算機（３１２０）である。４００２で、外部クライアント計算機（１０００）が発行した処理要求パケットが公共回線（２０００）経由で外部ルータ（３１１０）に送られてくる。４００３で、外部ルータ（３１１０）内の外部<;->;境界通信制御部（３１１１）のパケットフィルタリングが行われ、宛先やパケット種別が判断され正当性が確認された処理要求パケットは、境界サーバ計算機（３１２０）に送られてくる。ここで、もしパケットの正当性が不正な場合は処理を終了（４０１０）する。

【００２４】４００４で、境界サーバ計算機（３１２０）に届いた処理要求パケットは、境界サーバ計算機（３１２０）内の境界サーバ（３１２３）に送られ、クライアント指定処理対応部（３１２４）によって、パケット内容の確認と送り元の認証が行われ、正当性が確認されると、クライアント指定処理対応部（３１２４）から新たに内部ネットワーク（３２００）へ送るため、パケット変換や必要な認証処理が行われ、内部ルータ（３２１０）に対しパケットが発信する。ここでも、もしパケット内容の正当性が不正な場合や送り元の認証が失敗した場合は、処理を終了（４０１０）する。４００５で、内部ルータ（３２１０）内の内部<;->;境界通信制御部（３２１１）のパケットフィルタリングが行われ、変換後のパケット種別が判断されたり宛先の確認が行われ、正当性が確認されたパケットは、内部ネットワーク内に送られる。

【００２５】一方、パケット種別が不正であったり、宛先確認に失敗すると処理を終了（４０１０）する。４００６で、内部ネットワーク（３２００）に到着したパケットは、最終的に処理を実行する内部サーバ計算機（３２２０）や内部クライアント計算機（３２３０）に送られ、処理要求が実行される。以上が外部クライアント計算機（１０００）が、特定サイト（３０００）内の内部ネットワーク（３２００）へアクセスする時における、一連の通信処理流れである。

【００２６】ここで、図２の構成におけるセキュリティの問題点について述べる。

【００２７】一般的に、公共回線（２０００）、特定サイトのネットワーク内（３１００、３２００）を流れるパケットは内容の暗号化等が施されており、比較的盗聴等に遭った場合でも安全に設計されている。しかしながら、境界ネットワーク（３１００）上に存在する境界サーバ（３１２３）のベースとして動作するシステム（３１２２）は、一般的に流通ＯＳやミドルソフトウェアで構成されており、その内部構造等が解析され易い。また境界サーバ（３１２３）の役割としては、外からの情報を処理する他、情報を外部に発信する役目を持つ、必然的にパケットのフィルタリングという意味では、内部ルータ（３２１０）に比べ、外部ルータ（３１１０）のセキュリティレベルは低く設定されていることが多い。そのため、外部の不正な侵入者が境界ネットワーク（３１００）上の境界サーバ計算機（３１２０）への不正な侵入を試みたり、不正な解析プログラムを送り込んだりするのが容易である。

【００２８】不正侵入されたり不正プログラムを送り込まれた場合、送付されてくる処理要求パケット内容の解析や改竄、更には内部ネットワークへ送るパケットの解析や改竄が実行される。そして最終的に企業内などの内部ネットワークに侵入を許し、機密情報などの漏洩やウィルス等の送り込みが行われ甚大な被害を被ることが多い。無論その対策として、境界ネットワーク（３１００）の境界サーバ計算機（３１２０）上のシステム（３１２２）を、独自なシステムとして稼働することも可能である。ただし、その場合システムの上で動作するサーバを始めとするアプリケーションも全く独自なものを用意する必要があり、汎用性が著しく下がる。

【００２９】前記セキュリティ上の問題点を解決するため、境界ネットワーク（３１００）上の境界サーバ計算機（３１２０）に、図１で説明した本発明のシステム構成を適応した場合の構成図を図４に示す。

【００３０】図４の構成内容について説明を行う。１０００、１００１、１００２、１００３、２０００、３０００、３１００、３１１０、３１１１、３１２０、３１２１、３１２２、３１２２、３１２３、３１２４、３２００、３２１０、３２１１、３２２０、３２３０は図２で説明した構成と一緒である。３００は図１で説明した多重システム並列稼働カーネルである。３１２５は、外部クライアント（１０００）からの処理要求パケットを一時的に保存するための格納領域であるクライアント指定処理要求保存部。３１２６は境界サーバ計算機（３１２０）上で内部サーバ計算機（３２２０）との通信を行うためのインタフェースハードウェア。３１２７はクライアント指定処理要求保存部の内容監視と、システム（３１２２）の不正操作/侵入監視を行う監視システム。３３２１は内部サーバ計算機（３２２０）の通信を行うためのインタフェースハードウェア。３２２２は内部サーバ計算機（３２２０）上で稼働するシステム。３２２３は前記システム（３２２２）上で動作するサーバソフトウェアであり、内部サーバと呼ばれる。３２２４は監視システム（３１２７）の指示により、クライアント指定処理要求保存部（３１２５）から外部クライアント（１０００）からの処理要求パケットを取得するクライアント指定処理要求取得部。３２２５はクライアント指定処理要求取得部から処理要求パケットを受け取り、内部ネットワーク内の指定計算機に処理要求パケットを送るためのクライアン

ト指定処理内部ネットワーク対応部。３２２６は内部サーバ計算機(３２２０)上で境界サーバ計算機(３１２０)との通信を行うためのインタフェースハードウェア。３３００は内部サーバ計算機(３２２０)の通信インタフェースハードウェア(３３２６)と境界サーバ計算機(３１２０) の通信インタフェースハードウェア(３１２６)を結ぶネットワークである、専用ゲートウェイＬＡＮ。

【００３１】本構成の特徴は、境界サーバ計算機(３１２０)に、図１で説明した多重システム動作カーネル(３００)を採用したところである。前記多重システム動作カーネル(３００)は境界サーバ計算機(３１２０)起動時に、従来と同様なシステム(３１２２)の他、監視システム(３１２７)をロードする。これらは図１で説明した、システム割込制御部(３０１)、システムメモリ空間管理部(３０２)で実現される。また前記それぞれのシステムは、一台の計算機上で動作しているが、システム(３１２２)は境界ネットワーク(３１００)に、監視システム(３１２７)は専用ゲートウェイＬＡＮ(３３００)にと、それぞれ全く別々のネットワークに繋がっている。ハードウェア的にも、それぞれのシステムが管理する通信インタフェースハードウェア(３１２１、３１２６)は、他システム側のハードウェア情報を検知出来ないように構成されている。これは図１で説明した、ハードウェア割当制御部(３０５)で実現される。つまり、一台の計算機上で全く、別々のセキュリティレベルを持つ計算機が独立して混在した環境を構成しているのである。

【００３２】監視システム(３１２７)は、多重システム並列カーネル(３００)経由で、定期的にシステム(３１２２)側を監視する。このため、多重システム並列カーネル(３００)は、監視システム(３１２７)からの通信要求とその返答はアクセスを許可するが、逆のシステム(３１２２)からの通信要求は受け付けないような設定を施してある。これは図１で説明したシステム間内部通信制御部で実現される。もし、外部クライアント(１０００)からの処理要求パケットを、システム(３１２２)側が受信しているようであれば、監視システム(３１２７)が専用ゲートウェイＬＡＮ(３３００)経由で内部サーバ計算機(３２２０)に指示を送り、内部サーバ計算機(３２２０)が処理要求パケットを取得し、最終的に内部ネットワーク内の指定計算機に処理要求パケットを送る。

【００３３】また、境界サーバ計算機(３１２０)上のシステム(３１２２)に不正者が侵入したり、不正プログラム等が送り込まれた場合は、監視システム(３１２７)が検知し、更に多重システム並列カーネル(３００)に不正アクセスを試みられた場合にも、多重システム並列動作カーネル(３００)が検知し監視システム(３１２７)に通知され、監視システム(３１２７)の指示によりシステム(３１２２)側の終了/リブートが実行され、その通知が管理者に通知される。これは図１で説明したシステム起動終了制御部(３０４)により実現される。

【００３４】図５に図４の構成を使った外部クライアント計算機(１０００)が、特定サイト(３０００)内の内部ネットワーク(３２００)へアクセスする場合の通信処理流れを説明する。なお、境界サーバ計算機(３１２０)に処理要求パケットが送られてくるまでの処理は、図３と同様なので、それ以降の説明をここでは行う。５０００で処理が開始される。５００１で、境界サーバ計算機(３１２０)に届いた処理要求パケットは、境界サーバ計算機(３１２０)内の境界サーバ(３１２３)に送られ、クライアント指定処理対応部(３１２４)によって、パケット内容の確認と送り元の認証が行われ、正当性が確認されると、クライアント指定処理対応部(３１２４)からクライアント指定処理要求保存部(３１２５)に格納される。ここでも、もしパケット内容の正当性が不正な場合や送り元の認証が失敗した場合は、処理を終了(５０１０)する。５００２で、監視システム(３１２７)が多重システム並列動作カーネル(３００)経由で、クライアント指定処理要求保存部(３１２５)を確認し、処理要求パケットが存在する場合、パケット内容の確認を行い正当なパケットであれば、専用ゲートウェイＬＡＮ(３３００)経由で、内部サーバ(３２２３)上のクライアント指定処理要求取得部に、パケット取得の指示を出す。ここでも、もし内容の正当性が不正な場合は、処理を終了(５０１０)する。５００３で、クライアント指定処理要求取得部が、クライアント指定処理要求保存部(３１２５)から、処理パケットを取得し、そのパケットをクライアント指定処理内部ネットワーク対応部(３２２５)に送付する。５００４でクライアント指定処理内部ネットワーク対応部(３２２５)が、最終的に処理を実行する内部サーバ計算機(３２２０)や内部クライアント計算機(３２３０)に送り、処理要求が実行される。以上が本特許のシステム構成を利用した場合における、外部クライアント計算機(１０００)が、特定サイト(３０００)内の内部ネットワーク(３２００)へアクセスする時における、一連の通信処理流れである。

【００３５】以上で本発明の一実施例の説明を終わる。

【００３６】

【発明の効果】本発明は、単一計算機上で複数システムを同時並列稼働させる環境を利用し、同時並列稼働しているシステム同士のセキュリティをシステム自体の改造無しに確保する。また、例え１つのシステムに不正な侵入がされた場合でも、侵入されたシステム自身の終了/リブートを実行し、他のシステムへの二次的な影響を防止し、他のシステムに影響を及ぼさないセキュリティの確保が可能である。

【００３７】特にインターネット、イントラネット、エクストラネットを含む公共回線をバックボーン回線として使用するネットワークで、前記公共回線上のクライアントから特定サイト内へアクセスをする際の通信制御において、前記通信制御用び中継器のセキュリティ確保が

可能となる。

【図面の簡単な説明】

【図１】本発明のシステム構成図。

【図２】現在の公共回線越え通信制御の構成図。

【図３】現在の公共回線越え通信制御処理の流れ図。

【図４】本発明を公共回線越え通信制御に用いた場合の構成図。

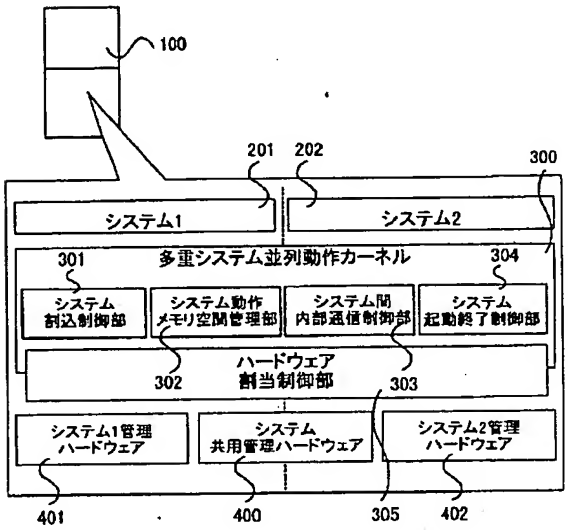
【図５】本発明による公共回線越え通信制御処理の流れ図。

【符号の説明】

１００…計算機、２０１…システム１、２０２…システム２、３００…多重システム並列動作カーネル、３０１…システム割込制御部、３０２…システム動作メモリ空間管理部、３０３…システム間内部通信制御部、３０４…システム起動終了制御部、３０５…ハードウェア割当制御部、４００…システム共用管理ハードウェア、４０１…システム１管理ハードウェア、４０２…システム２管理ハードウェア。

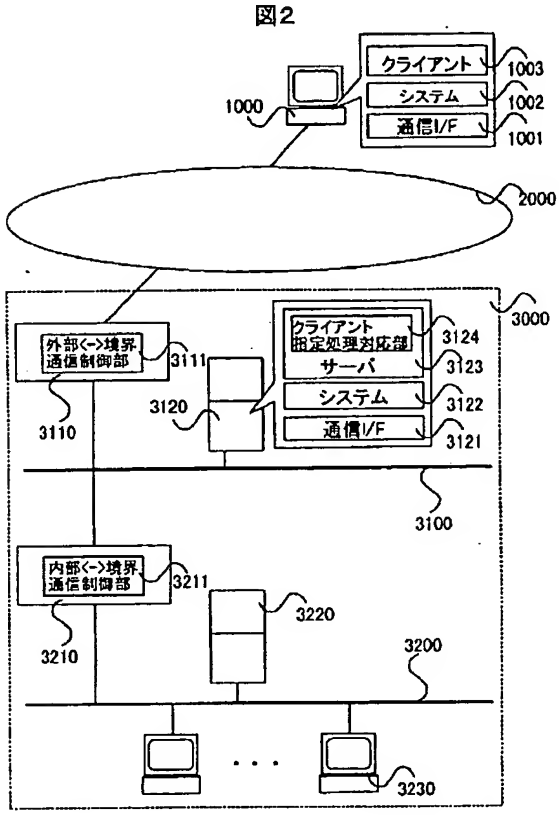
【図１】

図1



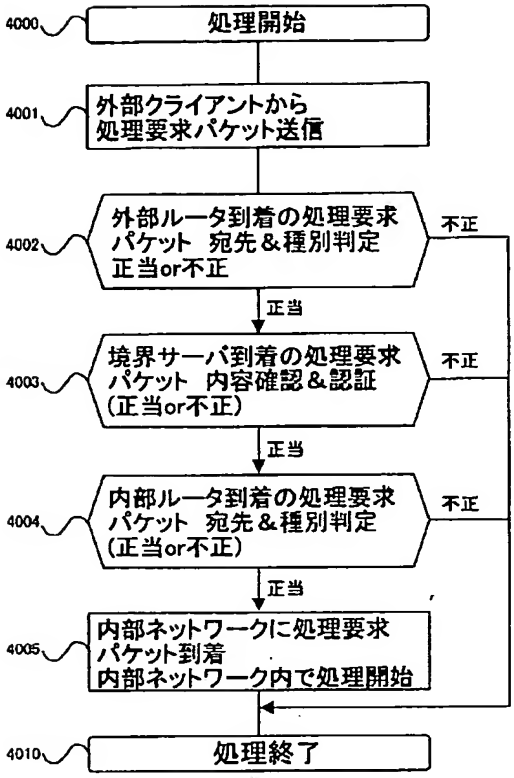
【図２】

図2



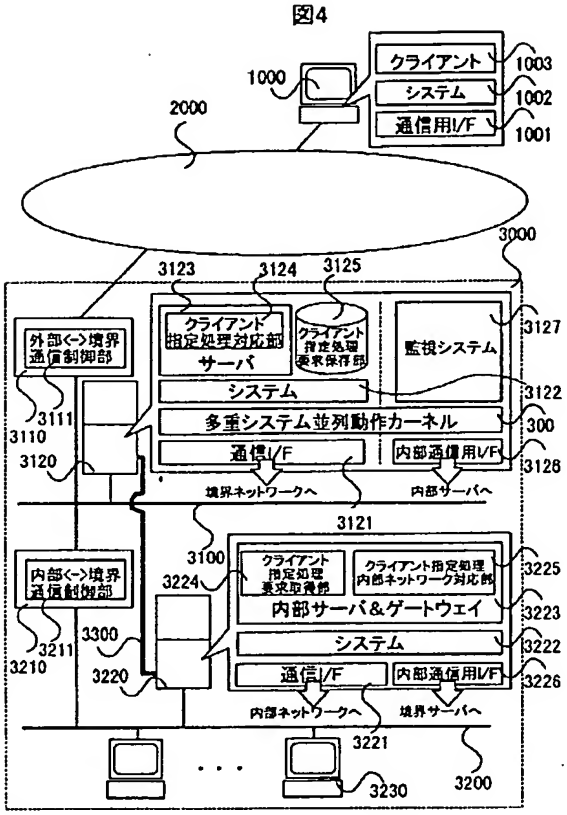
【図３】

図3


4000
処理開始
4001
外部クライアントから
処理要求パケット送信
4002
外部ルータ到着の処理要求
パケット　宛先＆種別判定
正当or不正
不正
正当
4003
境界サーバ到着の処理要求
パケット　内容確認＆認証
(正当or不正)
不正
正当
4004
内部ルータ到着の処理要求
パケット　宛先＆種別判定
(正当or不正)
不正
正当
4005
内部ネットワークに処理要求
パケット到着
内部ネットワーク内で処理開始
4010
処理終了

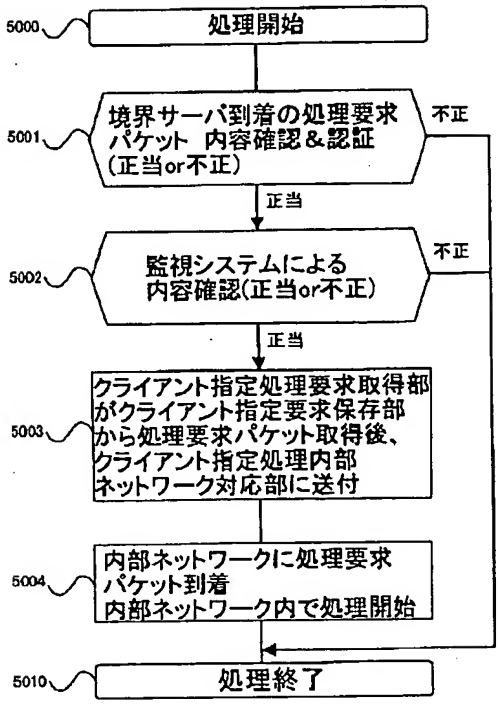
【図４】

図4


クライアント
システム
通信用I/F
1003
1002
1001
1000
2000
3000
3123
3124
3125
外部<->境界
通信制御部
クライアント
指定処理対応部
サーバ
クライアント
指定処理
要求保存部
監視システム
3127
システム
3122
多重システム並列動作カーネル
300
通信I/F
内部通信用I/F
3126
3111
3110
3120
境界ネットワークへ
内部サーバへ
3121
3100
内部<->境界
通信制御部
クライアント
指定処理
要求取得部
クライアント指定処理
内部ネットワーク対応部
3225
3224
内部サーバ＆ゲートウェイ
3223
3300
システム
3222
3211
3210
3220
通信I/F
内部通信用I/F
3226
内部ネットワークへ
境界サーバへ
3221
3230
3200

【図５】

図5



フロントページの続き

(72)発明者　大島　訓
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　内山　靖文
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内

Fターム(参考)　5B017 AA01 BA06 BA07 BB03 CA15 CA16
5B085 AE06 BG07
5B089 GA21 HA10 JB16 JB22 KA17 KB13 KC52 KC58 ME12